Dissuadindo o Terrorismo na Era da Informação

Tenente-Coronel (Res) Timothy L. Thomas, Exército dos EUA

O ATAQUE no dia 11 de setembro de 2001, contra os Estados Unidos, mudou radicalmente a maneira com que as nações e os organismos internacionais encaram o terrorismo. Por exemplo, o Presidente George W. Bush disse que os Estados Unidos dariam início a uma longa guerra contra o terrorismo e o Secretário de Defesa, Donald H. Rumsfeld, recebeu maiores créditos orçamentários para o combate ao mesmo. Pela primeira vez na história, a OTAN aplicou o Artigo 5 do Tratado de Washington de 1949, que reconhece que um ataque contra um membro da OTAN deve ser considerado como um ataque contra todos os membros da organização. Isto eliminou as restrições políticas normalmente associadas com o uso de força militar para combater o terrorismo. À medida que a investigação avançava, foi ficando aparente o poder das ferramentas da era da informação, tal como a Internet, para o planejamento e execução de atos terroristas.

A promessa de globalização decorrente da revolução da informação, o conseqüente menor custo das comunicações e a integração das economias possuem outra utilização, mais sinistra, quando em mãos de terroristas. Este artigo define o terrorismo na era da informação e examina de que maneira a informação permite ao terrorista dar prosseguimento à sua causa. Também são oferecidas recomendações para uma política de dissuasão para o combate a esta nova ameaça.[1]

Terrorismo na Informação

Tradicionalmente, o terrorismo enfatiza o uso da violência — para ameaças ou ações de fato — para causar o medo ou o alarme, geralmente com algum objetivo político em mente. Os terroristas exploram a estrutura formal do mundo civilizado para alcançar esses objetivos. Entre outras coisas, isso inclui a exploração das restrições legais e de inteligência de um estado/nação para agir; sua objetividade durante noticiários; e sua infra-estrutura e princípios operacionais. Quase tudo em um estado/nação encontra-se disponível ao exame e uso de seus cidadãos, e portanto, para o uso e exame do terrorista. O terrorista pode viver em praticamente total anonimato até cometer um crime ou ato de violência. Geralmente, ele se adestra nos próprios sistemas que usará para o ataque. Isto permite ao mais fraco enfrentar e combater o mais forte.

O terrorista vive em outro mundo, um mundo de sigilo quase total. Geralmente, existe pouca ou nenhuma informação a respeito de seus princípios operacionais e infra-estrutura de apoio. Ele não é sujeito a restrições em sua busca de informações ou na condução de atividades ilegais. Terroristas são criminosos que podem usar força indiscriminada contra as populações. Eles sabem que as reações da polícia ou militares podem ser limitadas devido às leis relativas às liberdades civis ou com a segurança. Os terroristas têm acesso às mesmas coisas que o cidadão comum e, como sanguessugas, vivem dos demais, dando vazão ao seu ódio. Seus métodos podem ser considerados assimétricos porque seu sistema de operações não se compara ao do mundo civilizado. A destruição dos edifícios do *World Trade Center* usando aeronaves como gigantescas bombas, com seus tanques cheios de combustível; o terror causado pelas cartas com antraz; o plano de explorar a indústria caminhoneira; o potencial uso de pequenos aviões para o transporte e espargimento de agentes químicos e biológicos; e o assassinato do líder da Aliança do Norte, no Afeganistão, com um explosivo escondido dentro de uma máquina fotográfica durante uma entrevista, são bons exemplos das ferramentas assimétricas disponíveis aos terroristas.

O FBI define o terrorismo como "o uso de força ou violência ilegal contra pessoas ou propriedade para intimidar ou coagir um governo, a população civil, ou qualquer outro segmento com a intenção de alcançar

objetivos políticos ou sociais".[2] Na era da informação, o terrorismo expandiu o seu campo de atuação e encontrou aliados em instrumentos, como a Internet, que facilitam seus esforços. Já se usa a expressão "terrorismo cibernético" para definir a exploração da Internet com propósitos terroristas, definindo-o como o elo de ligação entre o abuso e uso fraudulento de sistemas de informação por criminosos e a violência física do terrorismo; e o abuso intencional de um sistema de informação digital, rede, ou componente com o fim de apoiar ou facilitar uma campanha ou ação terrorista.[3] Ataques a sistemas de computação são os exemplos mais citados como "o uso da força ou violência" na era da informação, por terem se tornado os meios de ataque mais conhecidos. O agente especial do FBI, Mark Pollitt, define o terrorismo cibernético como sendo "ataques premeditados e politicamente motivados contra a informação, sistemas e programas de computação e dados, que resultam em violência contra alvos não combatentes por grupos subnacionais ou agentes clandestinos".[4] O terrorismo cibernético usa da violência virtual, que é tanto psicológica como real, para alcançar seus objetivos. Outros métodos de alteração de dados podem também ser considerados como terrorismo cibernético, tal como interferir nos sistemas de posicionamento global ou causar a colisão de duas aeronaves.

Departamento de Defesa

Durante uma missão de reconhecimento na Zhawar Kili, no leste do Afeganistão, Forças Especiais de Terra, Mar e Ar da Marinha dos EUA, os Navy Seals, encontraram valiosa informação de inteligência, incluindo este cartaz de propaganda de Osama bin Laden, colocado em uma sala de aula de terrorismo da Al-Qaeda. Também foi encontrado uma grande quantidade de munições em numerosas cavernas, e vários suspeitos membros da Al-Qaeda e do Talibã foram detidos.

A Internet e a "Guerra na Rede"

Talvez um termo mais apropriado para definir o terrorismo de hoje seja simplesmente "o terrorismo na era da informação" ao invés de terrorismo cibernético. Por exemplo, com relação à Internet, um terrorista tentará obter sucesso usando a sua idéia básica de facilitadora da integração e cooperação mundiais para desacreditar governos, degradar a autoconfiança do usuário, corromper ou interferir com sistemas importantes inserindo dados errôneos ou causando desconexões intermitentes. Em muitos casos, isto produz terror ou alarme e se torna um complemento contemporâneo do terrorismo tradicional. Existem nove maneiras mais prováveis de utilização da Internet por um grupo terrorista:

Dados sobre alvos sensíveis. A Internet pode ser usada para colher informações detalhadas sobre alvos. Se um terrorista obtém certas informações sobre um alvo importante, como um oleoduto ou sistema de energia, pode manipular ou fazer chantagem contra o comércio ou governos. Preocupação com o fácil acesso a imagens de alvos em potencial se tornaram aparentes logo após o dia 11 de setembro de 2001, quando vários sites na Internet removeram fotos e outras informações que, repentinamente, pareciam ser demasiado sensíveis. No dia 18 de outubro, o Pentágono adquiriu os direitos sobre as fotografias do Afeganistão tiradas pelo satélite *Ikonos* da *Space Imaging Incorporated*, que pode identificar objetos no solo de dimensões tão pequenas quanto de um metro quadrado.

Apoio financeiro. A Internet pode ser usada para a solicitação de fundos em apoio a alguma causa e para manipular opções nas bolsas de valores que beneficiem terroristas após um ataque. Um dos sites dedicados à causa da República da Chechenia, em sua luta para separar-se da Rússia encaminha visitantes a um banco e informa o número de uma conta para a qual estes podem enviar dinheiro para apoiar esse esforço. Atualmente, uma investigação procura descobrir se foram feitas negociações em bolsa de valores pela rede *al-Qaeda* nos dias precedendo 11 de setembro.

Conectando grupos diferentes. A Internet pode ser usada para conectar grupos diferentes. Uma seita religiosa de qualquer país ou região, ou pessoas que apóiam uma determinada causa, já podem se comunicar. Estes sites dão instruções a respeito de quando e onde ocorrerão reuniões ou sobre tipos de protestos ou assuntos que podem ser estudados. A Internet tem um efeito sinérgico sobre esse tipo de atividades.

Extorsão. A Internet pode ser usada para atacar indivíduos, grupos ou companhias, tais como instituições financeiras, ou para tentar influenciar os responsáveis

pelo processo de tomada de decisões. Extorsionários a usam para extorquir dinheiro de instituições financeiras sob ameaça de ataques cibernéticos ou da perda de credibilidade.

Publicidade. A Internet tem um potencial incalculável para a publicidade e é freqüentemente usada nesse sentido. Pode ser vista instantaneamente por uma audiência global. Um exemplo disso é o de Osama bin Laden, que usou a televisão e a Internet para disseminar a sua mensagem de morte a todos os americanos depois de iniciado o ataque da coalizão ao Afeganistão. Os Estados Unidos imediatamente pediram que não lhe fosse concedida mais publicidade. Grupos terroristas consideram a mídia como sendo a mais alta prioridade estratégica para a abordagem de suas causas.

A ex-Procuradora Geral da Justiça, Janet Reno, supostamente disse a um painel presidencial sobre o terrorismo em 2000, que grupos extremistas estão codificando tanto o correio eletrônico como mensagens faladas. Um israelita, o Dr. Reuven Paz, do Instituto de Contraterrorismo, acredita que todos os grupos terroristas estão usando a Internet para propagar as suas mensagens.

Liberdade global. Graças à Internet, o terrorismo já não é mais restrito ao estado em que se esconde. Elétrons não precisam de passaporte.[6] Na verdade, a base para operações terroristas já nem se encontra mais no país alvo das mesmas.

Efeitos psicológicos. A Internet pode ser usada para iniciar o terrorismo psicológico. Esse aspecto da Internet muitas vezes é ignorado. Não apenas pode ser usada para causar o pânico, devido à sua aparente credibilidade, mas também para a dissimulação ou para criar divisões.

Dissimulação. A Internet mudou a rede de comunicações terroristas — de uma apoiada em um centro de controle principal para uma sem centro de controle específico — devido à natureza de sua própria rede. Cúmplices, tais como os *hackers* podem ser usados, até mesmo sem perceberem que o estão sendo, para servirem aos propósitos do terrorismo sem compreenderem o resultado final de suas ações.

Operações secretas. A Internet pode ser usada para enviar mensagens clandestinas, tal como o uso de tinta invisível que a *al-Qaeda* promove como alternativa de baixa tecnologia às comunicações no ciberespaço. Por exemplo, existem indicações que peritos em computação egípcios, trabalhando no Afeganistão, idealizaram uma rede de comunicações que permite a extremistas o intercâmbio de informações via Internet sem temer serem detectados, o que poderia ocorrer se usassem o correio eletrônico ou boletins de mensagens eletrônicas tradicionais.[7] As atenções estão voltadas para esta última tática devido ao suposto uso da esteganografia (programa que oculta arquivos dentro de imagens) e codificação na Internet pelo grupo terrorista de bin Laden, a *al-Qaeda*.

O texto usado pelo Serviço de Mensagens Curtas (*Short Message Service — SMS*), é um texto oculto ou em código. Um exemplo seria, "ATQ 8 HJ", que poderia significar "ataque hoje às oito". Uma mensagem nesse formato pode ser enviada de um telefone celular a outro via um centro de *SMS*. O jornal *Hindustan Times*, da Índia, informou em novembro que notícias confiáveis ligavam o uso de técnicas *SMS* à *al-Qaeda* e outros grupos terroristas.[8] O *SMS* funciona com a transmissão de sinais desde um telefone celular ao centro operacional automático de *SMS* do usuário. O centro liga para o número do destinatário do *SMS* e coloca a mensagem em espera. Este método pode forçar os governos a monitorar os centros de *SMS*.

Um autor observa que, "se existe algo que o FBI odeia mais que Osama bin Laden, é quando este começa a usar a Internet."[9] Ele acusa bin Laden de esconder mapas, fotos de alvos e disfarçar instruções em áreas de bate-papo, boletins de mensagens em sítes pornográficos e em outros sites. Com a esteganografia, mensagens podem ser escondidas dentro de arquivos de áudio, vídeo, ou de imagens fixas, com a informação sendo arquivada nos mais insignificantes dígitos binários (*bits*) de um arquivo digitalizado.

O FBI e outras autoridades que atuam contra o terrorismo nos Estados Unidos acreditam que a organização de bin Laden já usou a esteganografia no passado. Até agora, ninguém afirmou que os terroristas que planejaram e executaram os eventos do dia 11 de setembro de 2001 usaram essa técnica. Poucos dias antes do ataque, uma equipe da Universidade de Michigan usou uma série de computadores em busca de imagens que pudessem conter planos terroristas, mas não encontraram nenhum. No entanto, investigadores do FBI descobriram centenas de mensagens de correio eletrônico, associadas aos edifícios do *World Trade Center*, enviadas desde bibliotecas e computadores pessoais. Foram escritas em inglês ou em árabe e não foram codificadas; podiam ser lidas abertamente.[10] Talvez o grupo de bin Laden tenha percebido que o FBI estava prestes a examinar as mensagens codificadas e decidido enviá-las em claro na esperança de que não fossem examinadas tão de perto.

A codificação, por outro lado, depende de códigos e cifras para embaralhar mensagens. Em um artigo recente

Departamento de Defesa

Um soldado do 1º Batalhão, 3º Grupo de Forças Especiais, dirige uma viatura QT para dentro de uma caverna à procura de munições nas aforas de Cabul, no Afeganistão, no dia 19 de julho de 2002.

no jornal *USA Today*, o autor cita um oficial norte-americano, anônimo, que assegura que a codificação tem se tornado "a ferramenta diária de extremistas muçulmanos no Afeganistão, Albânia, Inglaterra, Caxemira, Kosovo e outros lugares e que bin Laden e outros extremistas muçulmanos estão ensinando o método em seus campos no Afeganistão e no Sudão".[11] Em seu testemunho perante o Congresso, o antigo diretor do FBI, Louis J. Freeh, reclamou do uso da codificação, mas não da esteganografia. A ex-Procuradora Geral da Justiça, Janet Reno, supostamente disse a um painel presidencial sobre o terrorismo em 2000, que grupos extremistas estão codificando tanto o correio eletrônico como mensagens faladas. Um israelita, o Dr. Reuven Paz, do Instituto de Contraterrorismo, acredita que todos os grupos terroristas estão usando a Internet para propagar as suas mensagens. O problema das autoridades policiais é que a Internet tem, no momento, aproximadamente 28 bilhões de imagens e 2 bilhões de sites.

As redes de comunicações, em geral, têm recebido quase tanta atenção quanto a Internet nos últimos anos. Os autores David Ronfeldt e John Arquilla criaram o termo *netwar* (guerra na rede) há muitos anos. Esta refere-se ao "emergente modo de conflito no nível societário, sem chegar a ser uma guerra militar tradicional, no qual os protagonistas usam modelos de organização de redes de comunicações e doutrinas, estratégias e tecnologias relacionadas, sincronizadas à era da informação".[12] A *netwar*, então, parece ser uma versão atualizada da antiga organização celular comunista, uma rede de comunicações complexa em si,

Todas as nações, no nível internacional, devem cooperar com os tratados de assistência mútua legal, extradições, participação de inteligência, e leis uniformes relacionadas ao crime ligado à computação, para que as investigações e processos judiciais possam cruzar fronteiras internacionais.

que usava métodos de entrega sigilosas e clandestinas e intermediários na condução de operações. Em geral, foi a predecessora mais centralizada da *netwar* que Ronfeldt e Arquilla descrevem. Estas redes de comunicações oferecem não apenas os benefícios de integração, mas também vários riscos e perigos, incluindo ameaças à liberdade e privacidade, novos métodos de reconhecimento e muitas vulnerabilidades a nossa infra-estrutura de segurança nacional. Mais importante, as redes permitem que atores não estatais se constituam em redes

de comunicações multiorganizacionais, oferecendo aos que nada têm, uma oportunidade de trabalhar no mesmo nível com os que têm. [13]

Outro ponto excelente mencionado pelos autores é que a força de uma rede de comunicações depende de cinco níveis de funcionamento: organizacional (criação), narrativo (contar estórias), doutrinário (estratégias e métodos), tecnológico (sistemas de informação) e social (relacionamentos pessoais).[14] Aparentemente, a rede de comunicações *al-Qaeda* funcionou em todos estes níveis, durante o planejamento e execução dos ataques do dia 11 de setembro. A rede faz com que o grupo pareça não ter líder, e isto torna mais difícil encontrar os responsáveis.

No entanto, Ronfeldt e Arquilla parecem depender demasiado de sua descrição da doutrina militar conhecida por *swarming* para explicar o que deve ser feito para neutralizar as atividades terroristas nas redes de comunicações. Inclusive, ignoram seus próprios conselhos. Eles definem a doutrina como sendo uma forma estruturada, coordenada e estratégica de atacar, de todas as direções, um ponto ou pontos em particular por meio de fogo ou força contínuas.[15] Na realidade o *swarming* (da palavra *swarm* — enxame) não é muito diferente do velho conceito de massa. De fato, em um dos seus exemplos, citam estratégias críticas de massa empregadas por um grupo de protesto. Ainda mais significativamente, os autores, em sua confiança nessa doutrina, ignoram o seu nível doutrinário funcional, que recomenda o uso de estratégias e métodos. O *swarming* é o único oferecido, quando inúmeras outras opções deviam ser consideradas. Teorias, tais como os 36 estratagemas de guerra da China, e os princípios de guerra russos e norte-americanos, são apenas algumas das disponíveis. Estas últimas ofereceriam muito mais opções do que apenas o *swarming*, na forma de bloqueios, o uso de dissimulações e reconhecimento. As redes de comunicações não serão derrotadas por meio de "forçá-las à defensiva", como concluem os autores, mas pela execução de ataques de precisão contra seus sistemas funcionais. Os chineses, por exemplo, recomendariam o uso da "guerra de acupuntura", ou seja, ataques contra sistemas selecionados para paralisar um inimigo. Se fosse eficaz, um ataque em massa talvez nunca seja necessário.

Embora o terrorismo na era da informação esteja longe de ser resolvido, é encorajador ver o rápido desenvolvimento de métodos e procedimentos para combatê-lo. Este esforço deve ser ampliado e refinado nos meses vindouros e muitas opções de métodos de dissuasão devem ser discutidas. Por outro lado, é importante observar a dinâmica da opinião pública durante esse período. A cooperação e o entendimento entre os líderes podem ser a chave do sucesso no combate ao terrorismo.

Sugestões para a Dissuasão.

O que poderia ser feito para impedir o uso da Internet e das técnicas de guerra em rede por parte dos terroristas? O Dr. John Chipman diz que, referindo-se ao antigo sentimento de solidariedade emocional e à atual sobrecarga política compartilhada no combate ao terrorismo, "esperamos que seja feito o que for preciso com fineza econômica, experiência política, firmeza militar e determinação moral, tudo em um perfeito equilíbrio".[16] Chipman faz várias observações excelentes que oferecem uma idéia de um plano de dissuasão ao terrorismo:

- Um esforço diplomático é necessário para convencer os estados que apóiam o terrorismo a desistirem de tais atividades ou a sofrerem as conseqüências, tais com as sofridas pelo *Taliban* atualmente.
- Sanções comerciais poderiam ser impostas aos estados que têm ligações com terroristas.
- O combate ao terrorismo deve ser combinado com campanhas estratégicas de não proliferação, para manter certas armas fora do alcance desses grupos. Isto traria à mesa de negociações o debate entre o papel dos controles de exportação e da ação direta em oposição aos instrumentos de controle de armas, preferido por alguns.
- Os principais grupos terroristas devem ser caçados, não apenas os grupos locais.
- Devem ser desenvolvidas abordagens criativas à troca de informações, com atenção especial dada a países fora do Grupo dos Oito — os EUA, Reino Unido, França, Itália, Japão, Rússia, Canadá, e Alemanha — a OTAN e a União Européia. Isto inclui a troca de inteligência para a proteção da infra-estrutura crítica.
- Deve-se esperar protestos relacionados com direitos civis já que serão necessárias ferramentas de investigação até agora restritas, associadas com a Internet.
- Comandos militares de defesa da pátria terão maior autoridade sobre o relacionado à dissuasão terrorista.
- Grupos regionais, tal como a OTAN, devem considerar a eliminação das distinções entre áreas porque ataques cibernéticos podem vir de qualquer parte.
- Os principais bancos mundiais devem manter uma ação coordenada para fortalecer a credibilidade e equilibrar os mercados instáveis. Não se pode combater o terrorismo sem ter estabilidade.
- Elementos muçulmanos devem ajudar a organizar os

elementos atuais políticos da coalizão enquanto que os EUA e a Europa devem estar preparados para fornecer assistência econômica, física e técnica sem precedentes. Mais áreas do mundo em desenvolvimento devem ser incluídas no mundo moderno e pós-moderno.[17]

Todas as nações, no nível internacional, devem cooperar com os tratados de assistência mútua legal, extradições, participação de inteligência, e leis uniformes relacionadas ao crime ligado à computação, para que as investigações e processos judiciais possam cruzar fronteiras internacionais. A Assembléia Geral da ONU adotou a resolução 53/70 em dezembro de 1998, que convida membros a trocarem idéias sobre assuntos relacionados à segurança da informação e aos meios de combater o crime e o terrorismo relacionados à informação.[18] Tais medidas de dissuasão devem continuar a ser exploradas mais freqüentemente. Os terroristas exploram a objetividade e liberdade do mundo civilizado na defesa de suas causas. No passado, as ações terroristas eram mais difíceis de organizar e executar devido às distâncias e à dificuldade de coordenação. Hoje, essas considerações e muitos outros pormenores foram amenizados ou até mesmo eliminados, graças às ferramentas da era da informação, como a Internet. O resultado é o novo terrorismo em rede, coordenando doutrina, narrativa, organização e lealdade, freqüentemente em claro, por meio da tecnologia da esteganografia e codificação. Isto tem tornado os ataques terroristas mais eficazes, mais oportunos, e mais difíceis de serem detectados e denunciados pelas autoridades policiais.

Estes assuntos têm motivado os governos, ultimamente, a dedicarem tempo e dinheiro no combate ao terrorismo. A criação, recentemente, do Departamento de Segurança Interna nos EUA e a recente legislação, que permite às agências de polícia agirem mais rapidamente na apreensão de suspeitos de terrorismo, são duas das mais aparentes manifestações deste processo. Na área internacional, formaram-se alianças rapidamente para combater a nova ameaça, com a cooperação entre os EUA e a Rússia para resolverem assuntos relacionados com bases na Ásia Central sendo o melhor exemplo.

Embora o terrorismo na era da informação esteja longe de ser resolvido, é encorajador ver o rápido desenvolvimento de métodos e procedimentos para combatê-lo. Este esforço deve ser ampliado e refinado nos meses vindouros e muitas opções de métodos de dissuasão devem ser discutidas. Por outro lado, é importante observar a dinâmica da opinião pública durante esse período. A cooperação e o entendimento entre os líderes podem ser a chave do sucesso no combate ao terrorismo.***MR***

Referências

1. O autor acredita que a dissuasão é fundamental no combate ao terrorismo.
2. U.S. Department of Justice, *Terrorism in the United States* (Washington, DC: *Federal Bureau of Investigation*, 1998).
3. Matthew G. Devost, Brian K. Houghton, e Neal A. Pollard, "Information Terrorism: Can You Trust Your Toaster?" *The Terrorism Research Center* (abril de 1996), p.10.
4. Mark Pollitt, "Cyberterrorism—Fact or Fancy?" Resultados da XX Conferência de Segurança dos Sistemas de Informação Nacional (outubro de 1997), pp. 285-89.
5. Michael R. Gordon, "Pentagon Corners Output of Special Afghan Images," *The New York Times* (19 de outubro de 2001), B2.
6. Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," *The Terrorism Research Center*, data desconhecida, p.19, online no <www.terrorism.com/documents/denning-infoterrorism.html>.
7. John Arquilla, David Ronfeldt, e Michelle Zaninni, "Networks, Netwar, and Information Age Terrorism" em *Countering the New Terrorism* (Washington DC: RAND Corporation, 1998), pp. 65 e 66.
8. Saurabh Shukla, "Is Osama Using SMS to Brief his Sleeper Agents?" *Hindustan Times*, 11 de novembro de 2001, online no <Hindustantimes.com>.
9. Declan McCullagh, "Bin Laden: Steganography Master?" online no <http://www.wired.com>.
10. Duncan Campbell, "How the Plotters Slipped U.S. Net: Spy Networks Failed to Detect E-Mail and Satellite Conversations Used to Plot the Attack on the U.S.," *The Guardian* (27 de setembro de 2001).
11. Jack Kelley, "Terror Groups Hide Behind Web Encryption," *USA Today*, 6 de junho de 2001, online no <http://www.usatoday.com>.
12. David Ronfeldt e John Arquilla, "Networks, Netwars, and the Fight for the Future," *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Washington, DC: RAND 2001, TBP), conforme um correio eletrônico enviado ao autor.
13. *Ibid.*
14. *Ibid.*
15. *Ibid.*
16. John Chipman, "The Strategic Implications of Terror in the Information Age," Conferência Anual do Instituto Internacional de Estudos Estratégicos em Genebra, na Suíça, entre 12-15 de setembro 2001, online no <http://www.iiss.org/pub/tx/tx01015.asp>.
17. UN Resolution 53/70, O desenvolvimento no campo das informações e telecomunicações no contexto da segurança internacional (Nova Iorque: Resoluções de Desarmamento das Nações Unidas, 53ª Assembléia Geral, Nações Unidas, Departamento de Assuntos Econômicos e Sociais, dezembro de 1998).

O Tenente-Coronel (Res) Timothy L. Thomas é analista do Escritório de Estudos Militares Estrangeiros, no Forte Leavenworth, em Kansas, servindo também como professor adjunto no Instituto Europeu-Asiático do Exército dos EUA, localizado em Garmisch, Alemanha. Recebeu o título de Bacharel em Ciências pela Academia Militar do Exército dos EUA, em West Point; o de Mestre em Artes pela University of Southern California*, e é graduado da Escola de Comando e Estado-Maior do Exército dos EUA e do Instituto Russo do Exército norte-americano. Serviu em várias posições de comando e estado-maior no território continental dos EUA e na Europa. Dentre elas, foi Diretor do Departamento de Estudos Soviéticos do Instituto Russo do Exército dos EUA, em Garmisch. Seu artigo "IT Requirements for 'Policekeeping' " foi publicado no número de setembro-outubro de 2001 da* Military Review*, edição em inglês.*